SSH в NX-OS переключает Использование основанной на ключе аутентификации

Содержание

Введение

Этот документ описывает как к ssh в многоуровневый коммутатор данных (MDS) Cisco 9000 или коммутаторы Серии Nexus, не будучи предложенным для пароля пользователя Secure Shell (SSH).

Можно использовать ssh с основанными на ключе командами проверки подлинности и командами выполнения так, чтобы не было никаких приглашений пароля.

ssh switch# username@switch команда

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Сервер с приложением ssh, которое является текущим

Используемые компоненты

Сведения в этом документе основываются на сервере Linux с версией ssh:

Ssh $**-v**
OpenSSH_5.0p1-hpn13v1, OpenSSL 0.9.8d 28 сентября 2006

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Для активации этой опции, выполните эти шаги:

Шаг 1. SSH должен быть включен на коммутаторе MDS/Nexus.

```
#conf
(config)#feature ssh
```

Шаг 2. Необходимо получить открытый ключ от хоста и настроить его на коммутаторе MDS/Nexus.

Опции:

- v: многословный включил

- b: Количество Битов для ключа

T: Тип Алгоритма или DSA или RSA

```
$ ssh-keygen -v -b 1024 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/users/thteoh/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /users/thteoh/.ssh/id_rsa.
Your public key has been saved in /users/thteoh/.ssh/id_rsa.pub.
The key fingerprint is:
61:18:ad:14:cd:a7:bf:44:89:73:4a:2e:09:96:bb:51 thteoh@people
```

> **Примечание:** В данном примере используется RSA, можно также выбрать ключ Алгоритма цифровой подписи (DSA).

Проверьте генерируемую ключевую кошку использования с id_rsa.pub файлом (файл может также быть id_dsa.pub),

```
$ cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7obiQTKnT9+eH7h2
WCArEiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDu/3WP/ni4wJBb+yDqoI6+G1Rq/F2aYx45fh
6SwlPv0= thteoh@people
```

Шаг 3. Передайте id_rsa.pub (или id_dsa.pub), файл к каталогу загрузочной флэш-памяти MDS/Nexus коммутирует и настраивает открытый ключ ssh.

В этой экс-иноходи SFTP используется для передачи id_rsa.pub в коммутаторе MDS

```
#copy sftp:  bootflash
```

Для передачи файла в коммутаторах Nexus включают **VRF** в команду.

Шаг 4. . Генерируйте SSH-ключ на коммутаторе с помощью **id_rsa.pub** или **id_dsa.pub**.

для ссылки *teoh* имя пользователя используется.

```
#conf
(config)#username teoh sshkey file bootflash:id_rsa.pub
```

Шаг 5. . Можно проверить команду, завершенную успешно.

```
switch# show user-account teoh
```

```
user:teoh
this user account has no expiry date
roles:network-admin
ssh public key: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7o
biQTKnT9+eH7h2WCArEiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDu/3WP/ni4wJBb+yDqoI6+
G1Rq/F2aYx45fh6Swl
Pv0= thteoh@people
switch#
```

Проверка

Вы можете теперь ssh, чтобы коммутировать и выполнить любую команду без запроса пароля теперь:

```
$ ssh teoh@10.66.78.53 "sh system uptime"
Warning: the output may not have all the roles
System start time: Tue May 29 17:51:30 2012
System uptime: 7 days, 19 hours, 42 minutes, 15 seconds
Kernel uptime: 7 days, 19 hours, 45 minutes, 17 seconds
```